

What is claimed is:

1. A secure mail proxy system that is provided with a proxy server between a mail server on a LAN (Local Area Network) and the Internet for performing processing that is necessary for managing security such as
- 5 encryption and attachment of signatures to electronic-mail that is transmitted from said mail server to said Internet and decryption and detection of falsification of encrypted mail with attached signature that has been received from said Internet.
2. A secure mail proxy system according to claim 1 in which a proxy server is arranged between a mail server on a LAN (Local Area Network) and the Internet for carrying out processing relating to security of
- 5 electronic-mail, said proxy server comprising:
  - means for encrypting electronic-mail that has been received from said mail server, attaching a signature, and outputting to said Internet; and
  - means for, when encrypted mail with attached
  - 10 signature that is addressed to said mail server has been transmitted from said Internet, detecting whether or not falsification has occurred in said mail and, if no falsification has occurred, decrypting said encrypted mail and transmitting to said mail server;
  - 15 said secure mail proxy system being capable of

ensuring the security of electronic-mail on the Internet regardless of the type of mail server, mail client, or user terminal that is used by a user or whether or not security functions are incorporated in the mail server,  
20 mail client, or user terminal.

3. A secure mail proxy system according to claim  
1 wherein:

a proxy server is arranged between a mail server on a LAN (Local Area Network) and the Internet for  
5 carrying out processing relating to security of electronic-mail;

ordinary-text electronic-mail is transmitted from a mail client to said mail server; and

10 said mail server checks whether or not the destination of said electronic-mail is in said LAN and transmits electronic-mail that has a destination outside said LAN to said proxy server as ordinary text without alteration;

said proxy server comprising:

15 means for encrypting ordinary-text electronic-mail that has been received from said mail server such that only the mail recipient can decrypt said electronic-mail;

means for attaching a signature of the mail  
20 originator to encrypted mail and transmitting the

encrypted electronic-mail with attached signature to said Internet;

means for, in a case in which encrypted electronic-mail with attached signature has been transmitted by way of said Internet addressed to said mail server, checking whether said electronic-mail has been subjected to falsification, and if said electronic-mail has not been subjected to falsification, decrypting and converting said encrypted mail to ordinary-text mail

and delivering to said mail server; and

means for, in a case in which said electronic-mail has been subjected to falsification, rejecting the reception of said electronic-mail to prevent the entry of falsified electronic-mail into said LAN;

wherein said mail client requests said mail server for received electronic-mail and obtains ordinary-text electronic-mail from said mail server.

4. A secure mail proxy system according to claim 3 wherein said mail client is either connected directly to said LAN or is connected to said mail server of said LAN by way of at least one of a public line network, a radio-communication network, and a cable television (CATV) network.

5. A secure mail proxy system according to claim

1 that includes: a LAN (Local Area Network); a mail  
server that is connected to said LAN; and a proxy server  
provided between said mail server and the Internet for  
5 performing processing relating to electronic-mail  
security;

said proxy server comprising:

a secret key storage means for storing  
combinations of electronic-mail addresses and secret keys

10 that correspond to these electronic-mail addresses;

a public key storage means for storing  
combinations of electronic-mail addresses and public keys  
that correspond to these electronic-mail addresses;

wherein:

15 said secret keys are used when attaching to  
electronic-mail the signature of the originator and when  
decrypting encrypted mail that has been transmitted in  
addressed to an electronic-mail address in said LAN; and  
said public keys are used when encrypting mail

20 such that only the user of the electronic-mail address  
that is designated in the electronic-mail destination can  
read the encrypted mail and when checking whether mail  
has been falsified;

25 said proxy server being further provided with  
a data processor that includes:

mail encryption means for obtaining from said  
public key storage means the public key that corresponds

to the electronic-mail address of the electronic-mail destination and encrypting ordinary-text mail from said  
30 mail server using said public key;

mail signature attaching means for obtaining from said secret key storage means the secret key that corresponds to the mail address of the electronic-mail originator, calculating a message digest of said  
35 electronic-mail, and, after encrypting the calculated values using said secret key, attaching the encrypted values as the signature of the electronic-mail originator;

mail decryption means for obtaining from said  
40 secret key storage means the secret key that corresponds to the electronic-mail address of the electronic-mail destination, and decrypting encrypted mail using said secret key;

mail signature checking means for checking  
45 whether or not mail has been falsified by obtaining from said public key storage means the public key that corresponds to the mail address of an electronic-mail originator, decrypting the signature that is attached to mail using said public key; and comparing values of the  
50 signature with the message digest of the mail; and

data communication means for receiving ordinary-text electronic-mail from said mail server,  
transmitting encrypted mail with attached signature that

has been created by said mail encryption means and said  
55 mail signature attaching means to said Internet, and  
further, receiving encrypted mail with attached signature  
from said Internet and transmitting ordinary-text mail  
that is obtained by way of said mail signature checking  
means and said mail decryption means to said mail server.

6. A secure mail proxy system according to claim  
5 wherein said mail client is either connected directly  
to said LAN or is connected to said mail server of said  
LAN by way of at least one of a public line network, a  
5 radio-communication network, and a cable television  
(CATV) network.

7. A secure mail proxy system according to claim  
5 wherein said proxy server is not provided with: a  
secret key storage means for storing combinations of  
electronic-mail addresses and secret keys that correspond  
5 to the electronic-mail addresses, and a public key  
storage means for storing combinations of electronic-mail  
addresses and public keys that correspond to the  
electronic-mail addresses; but rather:

    said secure mail proxy system is provided  
10 with: an independent key management server for managing  
combinations of electronic-mail addresses and secret keys  
that correspond to the electronic-mail addresses; and an

independent directory server for managing combinations of electronic-mail addresses and public keys that correspond  
15 to the electronic-mail addresses;

wherein said mail encryption means, said mail signature attaching means, said mail decryption means, and said mail signature checking means of said proxy server each access said directory server and said key management server and obtain public keys and secret keys.

8. A proxy server that is arranged between a mail server that is connected to a LAN (Local Area Network) and the Internet for performing processing relating to electronic-mail security; is provided with:

5 a storage device that includes:  
a secret key storage section for storing combinations of electronic-mail addresses and secret keys that correspond to the electronic-mail addresses; and  
a public key storage section for storing  
10 combinations of electronic-mail addresses and public keys that correspond to the electronic-mail addresses;  
wherein said secret keys are used when attaching the signature of an originator to electronic-mail and when decrypting encrypted electronic-mail that  
15 has been transmitted in to an electronic-mail address in said LAN; and  
said public keys are used when encrypting mail

such that only the user of the electronic-mail address  
that is designated in the electronic-mail destination can  
20 read the encrypted mail and when checking whether mail  
has been falsified;

    said proxy server being further provided with  
    a data processor that includes:

    mail encryption means for obtaining from said  
25 public key storage section the public key that  
    corresponds to the electronic-mail address of the  
    electronic-mail destination and encrypting ordinary-text  
    mail from said mail server using said public key;

    mail signature attaching means for obtaining  
30 from said secret key storage section the secret key that  
    corresponds to the mail address of an electronic-mail  
    originator, calculating a message digest of said  
    electronic-mail, and, after encrypting the calculated  
    values using said secret key, attaching the encrypted  
35 values as the signature of the electronic-mail  
    originator;

    mail decryption means for obtaining from said  
    secret key storage section the secret key that  
    corresponds to the electronic-mail address of the  
40 electronic-mail destination, and decrypting encrypted  
    mail using said secret key;

    mail signature checking means for checking  
    whether or not mail has been falsified by obtaining from

45        said public key storage section the public key that  
corresponds to the mail address of an electronic-mail  
originator, decrypting the signature that is attached to  
electronic-mail using said public key; and comparing  
values of the signature with the message digest of the  
electronic-mail; and

50            data communication means for receiving  
ordinary-text electronic-mail from said mail server,  
transmitting encrypted mail with attached signature that  
has been created by said mail encryption means and said  
mail signature attaching means to said Internet, and  
55            further, receiving encrypted mail with attached signature  
from said Internet and transmitting ordinary-text mail  
that is obtained by way of said mail signature checking  
means and said mail decryption means to said mail server.

9.        A method of managing security of electronic-  
mail that is transmitted and received between a mail  
server and the Internet in which a proxy server is  
provided between a mail server on a LAN (Local Area  
5 Network) and the Internet for performing processing  
relating to electronic-mail security, comprising steps in  
which:

10            said proxy server encrypts and attaches a  
signature to electronic-mail that is to be transmitted to  
said Internet; and

said proxy server checks for falsification of  
electronic-mail that is addressed to said mail server  
from said Internet and decrypts said electronic-mail;

      wherein processes necessary for managing

15 security of electronic-mail are performed by said proxy  
server that is arranged at the point of connection to  
said Internet;

      whereby the security of electronic-mail on the  
Internet can be ensured regardless of the type of mail

20 server, mail client, or user terminal that is used by the  
user and regardless of whether the mail server, mail  
client or user terminal used by the user incorporates  
security functions.

10. A method of managing security of electronic-  
mail according to claim 9 wherein a proxy server is  
arranged between a mail server that is connected to a LAN  
(Local Area Network) and the Internet; comprising steps

5 in which:

      said mail server that has received ordinary-  
text electronic-mail from a mail client checks whether or  
not the destination of said electronic-mail is within  
said LAN and transmits electronic-mail having a

10 destination outside said LAN to said proxy server as  
ordinary-text without alteration;

      said proxy server encrypts ordinary-text

electronic-mail that is sent from said mail server such  
that only the mail recipient can decrypt said electronic-

15 mail;

the signature of the mail originator is  
attached and the encrypted electronic-mail with attached  
signature is transmitted to the Internet;

when encrypted electronic-mail with attached

20 signature has been transmitted in over said Internet  
addressed to said mail server, said proxy server checks  
whether or not said electronic-mail has been falsified;

if said electronic-mail has not been falsified,  
said encrypted electronic-mail is decrypted to ordinary-

25 text mail and then delivered to said mail server;

if said electronic-mail has been falsified,  
the reception of said electronic-mail is rejected to  
prevent entry of the falsified electronic-mail into said  
LAN; and

30 said mail client is used by the user to  
request said mail server for received electronic-mail and  
to receive ordinary-text electronic-mail from said mail  
server.

11. A method of managing security of electronic-  
mail according to claim 9, wherein the step in which said  
proxy server encrypts and attaches a signature to  
electronic-mail that is to be transmitted to said

- 5 Internet includes steps in which:
- a user uses a mail client to create electronic-mail and send the electronic-mail to a mail server as ordinary text without alteration;
- said mail server checks whether or not the
- 10 destination of electronic-mail that has been transmitted from said mail client is within the LAN (Local Area Network) to which said mail server is connected;
- ordinary-text electronic-mail is delivered to said proxy server when the destination of said
- 15 electronic-mail is outside said LAN;
- said proxy server receives ordinary-text electronic-mail from said mail server, obtains the public key that corresponds to the electronic-mail address of the destination of said electronic-mail from a public key
- 20 storage section that stores combinations of electronic-mail addresses and corresponding public keys that correspond to electronic-mail addresses, and encrypts said ordinary-text electronic-mail using the public key;
- said proxy server obtains the secret key that
- 25 corresponds to the electronic-mail address of the originator of said electronic-mail from a secret key storage section that stores combinations of electronic-mail addresses and secret keys that correspond to the electronic-mail addresses, calculates a message digest of
- 30 said electronic-mail, encrypts these calculated values

using the secret key, and attaches these encrypted values to said electronic-mail as the signature of the originator; and

said proxy server sends encrypted mail with

35 attached signature to the Internet.

12. A method of managing security of electronic-mail according to claim 9 wherein the step in which said proxy server checks for falsification of electronic-mail addressed to said mail server from said Internet and

5 decrypts said electronic-mail includes steps in which:

said proxy server receives encrypted electronic-mail with attached signature from said Internet;

said proxy server obtains from said public key

10 storage section the public key that corresponds to the mail address of the electronic-mail originator and decrypts the signature attached to said electronic-mail with said public key;

falsification of said electronic-mail is

15 checked by comparing values of the signature with the message digest of said electronic-mail;

if said electronic-mail has not been falsified,

said proxy server obtains from said secret key storage section the secret key that corresponds to the mail

20 address of the destination of said electronic-mail and

decrypts said electronic-mail using said secret key;  
electronic-mail that has been decrypted to  
ordinary text is delivered to said mail server in said  
LAN;

25 if said electronic-mail has been falsified,  
said proxy server rejects the reception of the mail to  
prevent entry of falsified electronic-mail into said LAN;  
said mail server receives ordinary-text  
electronic-mail from said proxy server; and

30 the user uses said mail client to request said  
mail server for mail that has been received and receives  
ordinary-text mail from said mail server.

13. A recording medium on which is recorded a  
program for performing processing relating to security of  
electronic-mail between a mail server that is connected  
to a LAN (Local Area Network) and the Internet using a  
5 proxy server;

wherein a storage device is provided that is  
in turn provided with:

a secret key storage section for storing  
combinations of electronic-mail addresses and secret keys  
10 that correspond to these electronic-mail addresses, and  
a public key storage section for storing  
combinations of electronic-mail addresses and public keys  
that correspond to these electronic-mail addresses;

5  
10  
15  
20  
25  
30  
35

wherein said secret key is used when attaching  
15 to electronic-mail the signature of the originator and  
when decrypting encrypted mail that has been transmitted  
in to an electronic-mail address in said LAN; and  
said public key is used when encrypting  
electronic-mail such that only the user of the  
20 electronic-mail address that is designated in the  
destination of the electronic-mail can read said  
electronic-mail and when checking for falsification of  
electronic-mail;

a program being recorded on said recording  
25 medium for causing a computer that constitutes said proxy  
server to execute the following processes from (a) to  
(e):

(a) a mail encrypting process in which the  
public key that corresponds to the electronic-mail  
30 address of the destination of electronic-mail is obtained  
from said public key storage section and ordinary-text  
mail is encrypted using the public key;

(b) a mail signature attaching process in  
which the secret key that corresponds to the mail address  
35 of the originator of electronic-mail is obtained from  
said secret key storage section, a message digest of said  
electronic-mail is calculated; the calculated values are  
encrypted using the secret key and the encrypted values  
are attached to electronic-mail as the signature of the

40 originator;

(c) a mail decryption process in which the secret key that corresponds to the electronic-mail address of the electronic-mail destination is obtained from said secret key storage section and encrypted mail  
45 is decrypted using the secret key;

(d) a mail signature checking process in which the public key that corresponds to the mail address of the originator of electronic-mail is obtained from said public key storage section, a signature that is attached  
50 to mail is decrypted using the public key, and falsification of mail is checked by comparing values of the signature and the message digest of the mail; and

(e) a data communication process in which ordinary-text mail is received from said mail server,  
55 encrypted mail with attached signature is transmitted to the Internet, encrypted mail with attached signature is received from said Internet, and ordinary-text mail is transmitted to said mail server.